UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/524,416 | 01/09/2006 | Hermann Sterzinger | 87305.00045 | 4455 |

30734 7590 02/01/2010

BAKER & HOSTETLER LLP
WASHINGTON SQUARE, SUITE 1100
1050 CONNECTICUT AVE. N.W.
WASHINGTON, DC 20036-5304

| EXAMINER | |
|---|---|
| JIANG, YONG HANG | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2612 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 02/01/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@bakerlaw.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/524,416 | STERZINGER ET AL. | |
| | Examiner | Art Unit | |
| | YONG HANG JIANG | 2612 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/6/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Objections*

Claim 11 objected to because of the following informalities: "and indication" on line 5.

Claim 13 objected to because of the following informalities: "wile" on line 3 and "al signal" on line 3 from the last.

Claim 27 objected to because of the following informalities: "said sidewa3]s" on line 4.

Claim 29 objected to because of the following informalities: "n complete" on line 3.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claims 11-12, 36-51, 53-56, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 36, 44, and 53, the claims are mistakenly written to be dependent on themselves.

Claims 37-43, 45-51, 55-56 depend on claim 36; Claim 54 depends on claim 53; therefore, they suffer the same deficiency.

Claim 11 recites the limitation "said an unauthorized interruption" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites the limitation "said host computer" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 44 recites the limitation "said host computer" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 53 recites the limitation "the door lock" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-2, 4, 35-37, and 56 are rejected under 35 U.S.C. 102(b) as being anticipated by Kim (US 6,040,771).

Regarding claim 1, Kim discloses a container manager, comprising: a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement (See Fig. 1);

a port borne by said housing to accommodate conduction of transmission of data signals between said closed interior and an environment external to said housing (via communication device 18, Col. 3, lines 22-26);

a control stage comprised of a memory storing information specific to said container (via control stage comprising CPU 220 and memory 204, Col. 3, lines 42-47) said control stage being mounted on said container, and being operationally coupled to provide communication with said interior via said port (Fig. 1), and generating a control signal in dependence upon disposition of said port relative to a source of said data signals (via CPU 220 detecting signals from communication device 250 to open or close lock, Col. 3, lines 51-53, Col. 4, line 66 to Col. 5, lines 5), in dependence upon disposition of said container within a scheme for generation of said data signals (via safe system 10 locked and secured), and in response to occurrence of a coincidence between a data key received among said data signals via said port (via remote control functions to open or close lock using the correct code, Col. 4, line 66 to Col. 5, lines 5) and a data sequence obtained by said control stage in dependence upon said information stored within said memory (via acceptable access numbers stored in memory ram 204, Col. 3, lines 42-47); and a moveable latch disposed to engage said lid and hinder removal of said lid from said complete engagement (via lock on door 14, Col. 3, lines 18-20), and to respond to said control signal by releasing said lid from said complete engagement (via lock on door 14 may be unlocked in response to correct code received, Col. 5, lines 1-5).

Regarding claim 2, Kim discloses a socket mounted within said housing providing said port (Fig. 1).

Regarding claim 4, Kim discloses an antenna mounted within said housing providing said port (via communication device 18 may comprise an antenna, See Col. 3, lines 22-27).

Regarding claim 35, Kim discloses the structural elements of the claimed invention (See rejection on claim 1 above), wherein Kim further discloses a source of an input signal representing a first class of information, mounted upon and borne by said housing (via input signals form sensors detecting abnormal conditions, Col. 4, lines 1-12); and a controls stage comprised of memory storing a second class of information specific to said container (via stored access numbers, Col. 3, lines 42-47).

Regarding claim 36, Kim discloses said source detecting movement of said lid, and said first class of information indicating said movement. (via horizontal detection sensor 234 detecting container including lid movement, Col. 4, lines 1-12).

Regarding claim 37, Kim discloses said source detecting a position of said lid, and said first class of information indicating said position (via horizontal detection sensor 234 detecting container including lid position change, Col. 4, lines 1-12).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Whiteside (US 5,835,861).

Regarding claim 3, Kim discloses the port may be wireless (See Col. 1, lines 22-27), but did not specifically disclose an infrared receiver mounted within said housing providing said port.

Whiteside teaches using infrared transmitters to broadcast a signal from one device to another device. (See Col. 2, lines 13-19)

From the teachings of Whiteside, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include an infrared receiver mounted within said housing providing said port as taught by Whiteside to use infrared wireless technology to broadcast/receive a signal from one device to another device, as it is well known infrared signals are less likely to be picked up by unauthorized receivers because infrared signals are direction based, thereby making wireless communication more secured.

4. Claims 5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Holtkamp (WO 00/76378).

Regarding claim 5, Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally through a data cable (via line connector). (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data key; and a data cable coupling said host computer to said port.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a microprocessor based host computer operationally coupled to said

controller via said port, generating said data key; and a data cable coupling said host computer to said port as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

Regarding claim 7, Kim discloses said port comprising a first antenna mounted within said container (via communication device 18 may comprise an antenna, See Col. 3, lines 22-27); a data transceiver connecting said first antenna and said controller (via transceiver device 226, col. 3, lines 48-51). Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally through a data cable (via line connector). (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data key.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a microprocessor based host computer operationally coupled to said controller via said port, generating said data key as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

The combination of Kim and Holtkamp did not specifically disclose a second antenna driven by said host computer, operationally connecting said host computer to said first antenna. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include a second antenna driven by said host computer, operationally connecting said host computer to said first antenna in order to use wireless communication between said container and said host computer, thereby making communication easier without the hassle of wires.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Holtkamp (WO 00/76378) and Cayne et al. (US 6,806,807).

Regarding claim 6, Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally through a data cable (via line connector). (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data key.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of

Kim to include a microprocessor based host computer operationally coupled to said controller via said port, generating said data key as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

The combination of Kim and Holtkamp did not specifically disclose a local area network coupling said host computer to said port. Cayne teaches using a local area network to couple a container manager to a host computer (See Fig. 8; and Col. 8, lines 19-21). From the teachings of Cayne, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include a LAN for data communication, thereby reliably send/receive data to the container manager.

6. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Holtkamp (WO 00/76378) and Whiteside (US 5,835,861).

Regarding claims 8 and 9, Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally through a data cable (via line connector). (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data key

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock

in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a microprocessor based host computer operationally coupled to said controller via said port, generating said data key as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

Kim discloses said port comprising a first antenna mounted within said container for wireless communication (via communication device 18 may comprise an antenna, See Col. 3, lines 22-27). But Kim did not specifically disclose an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data key; and an infrared receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter.

Whiteside teaches using infrared transmitters to broadcast a signal from one device to another device. (See Col. 2, lines 13-19)

From the teachings of Whiteside, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter, and to transmit operational communications

from said controller to said host computer via said firs infrared transmitter and receiver as taught by Whiteside to use infrared wireless technology to broadcast/receive a signal from one device to another device, as it is well known infrared signals are less likely to be picked up by unauthorized receivers because infrared signals are direction based, thereby making wireless communication more secured.

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Mogi et al. (JP 06085912 A).

Regarding claim 10, Kim teaches using sensors to detect abnormal conditions (See Col. 4, lines 1-12). But Kim did not specifically disclose said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port; and an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal.

Mogi teaches a communications line sensor to detect unauthorized interruption of the communication line. (See the Abstract)

From the teachings of Mogi, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port; and an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal in order to prevent theft or tampering of the safe system, thereby improving security.

8. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi, and further in view of Holtkamp (WO 00/76378)

Regarding claims 11-12, Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally. (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, periodically making a determination of whether said an unauthorized interruption of said communication has occurred; and an alarm driven by said host computer to broadcast an indication of said unauthorized interruption dependence upon said determination. Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be operated by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract) From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Mogi to include a microprocessor based host computer operationally coupled to said controller via said port as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient; periodically making a determination of whether said an unauthorized interruption of said communication has occurred; and an alarm driven by said host computer to broadcast an indication of said unauthorized interruption dependence upon said determination in order to monitor the container manager, thereby improving security.

9. Claims 13-14, 16, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim (6,040,771), and further in view of Mogi et al. (JP 06085912 A).

Regarding claim 13, Kim discloses a container manager, comprising: a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior wile said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement (See Fig. 1); a port mounted within said housing to receive data signals (via communication device 18, Col. 3, lines 22-26); a control stage comprised of a memory storing information specific to said container (via control stage comprising CPU 220 and memory 204 storing access numbers, Col. 3, lines 42-47), said control stage being mounted entirely within said container, being completely encased by said container during said complete engagement (fig. 1), and being operationally coupled to provide communication by data signals with said interior via said port (via communication device 18, Col. 3, lines 22-26). Kim teaches using sensors to detect abnormal conditions (See Col. 4, lines 1-12). But Kim did not specifically disclose said control stage generating a signal in response to an unauthorized interruption of said communication via said port; and an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal. Mogi teaches a communications line sensor to detect unauthorized interruption of the communication line. (See the Abstract)

From the teachings of Mogi, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to

include said control stage generating a signal in response to an unauthorized interruption of said communication via said port; and an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal in order to prevent theft or tampering of the safe system, thereby improving security.

Regarding claim 14, Kim discloses a socket mounted within said housing providing said port (Fig. 1).

Regarding claim 16, Kim discloses an antenna mounted within said housing providing said port (via communication device 18 comprising an antenna, Col. 3, lines 22-27).

Regarding claim 22, Kim discloses said controller generating a control signal in response to occurrence of a coincidence between a data key received via said port (via code received remotely, Col.4, line 66 to Col. 5, line 6) and a data sequence obtained by said control stage in dependence upon information stored within said memory (via access codes stored in memory, Col. 3, lines 42-47); and an electromechanical latch responding to said control signal by hindering removal of said lid from said complete engagement (via remote locking).

10. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi as applied to claim 13 above, and further in view of Whiteside (US 5,835,861).

Regarding claim 15, Kim discloses said port comprising wireless receiver (See col. 3, lines 22-27), but did not specifically disclose an infrared receiver mounted within

said housing providing said port. Whiteside teaches using infrared transmitters to broadcast a signal from one device to another device. (See Col. 2, lines 13-19)

From the teachings of Whiteside, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim and Mogi to include an infrared receiver mounted within said housing providing said port as taught by Whiteside to use infrared wireless technology to broadcast/receive a signal from one device to another device, as it is well known infrared signals are less likely to be picked up by unauthorized receivers because infrared signals are direction based, thereby making wireless communication more secured.

11. Claims 17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi as applied to claim 13 above, and further in view of Holtkamp (WO 00/76378).

Regarding claims 17 and 20, Kim teaches the use of a data cable (via data line, See Kim, Col. 3, lines 22-27) on the container manager, but the combination of Kim and Mogi did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals; and a data cable coupling said host computer to said port while conveying said data signals to said controller via said port.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract). From the teachings of

Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals; and a data cable coupling said host computer to said port while conveying said data signals to said controller via said port as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi as applied to claim 13 above, and further in view of Cayne et al. (US 6,806,807).

Regarding claim 18, the combination of Kim and Mogi discloses the structural elements of the claimed invention (see rejection on claim 13 above), but did not specifically disclose a local area network coupling a microprocessor based host computer to said port while conveying said data signals to said controller via said port. Cayne teaches using a local area network to couple a container manager to a host computer (See Fig. 8; and Col. 8, lines 19-21). From the teachings of Cayne, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Mogi to include a local area network coupling a host computer to said port while conveying said data signals to said controller via said port, thereby reliably send/receive data to the container manager and remotely controlling the container manager from a host computer.

13. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi as applied to claim 13 above, and further in view of Holtkamp (WO 00/76378).

Regarding claim 19, Kim discloses said port comprising a first antenna mounted on one of said sidewalls; data transceiver connecting said first antenna and said controller (via communication device 18 comprising antenna, Col. 3, lines 22-27). But the combination of Kim and Mogi did not specifically disclose a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals. Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract) From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient. The combination of Kim, Mogi, Holtkamp did not specifically disclose a second antenna driven by said host computer, operationally connecting said host computer to said first antenna wile conveying said data signals to said controller via said first antenna. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim, Mogi,

Holtkamp to include a second antenna driven by said host computer, operationally connecting said host computer to said first antenna wile conveying said data signals to said controller via said first antenna in order to provide wireless communication.

14. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Mogi as applied to claim 13 above, and further in view of Whiteside (US 5,835,861) and Holtkamp (WO 00/76378).

Regarding claim 21, claim 21 is the equivalent of claims 15 and 19 combined, therefore, claim 21 is rejected for the same reasons as claims 15 and 19.

15. Claims 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim (6,040,771), and further in view of Holtkamp (WO 00/76378).

Regarding claim 23, Kim discloses a container manager, comprising: a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement (See Fig. 1);

a port to receive data signals (via communication device 18, Col. 3, lines 22-26);

a control stage comprised of a memory (via control stage comprising CPU 220 and memory 204, Col. 3, lines 42-47), said control stage being mounted on said container and being operationally coupled to provide communication with said interior via said port (Fig. 1), and generating a control signal in response to occurrence of a coincidence between a data key received among said data signals via said port and a data sequence obtained by said control stage in dependence upon information stored

within said memory (via CPU 220 detecting signals from communication device 250 to open or close lock, the signal received matching acceptable access numbers stored in memory ram 204, Col. 3, lines 51-53, Col. 4, line 66 to Col. 5, lines 5, and Col 3, lines 42-47); and an electromechanical latch disposed to engage said lid and hinder removal of said lid from said complete engagement (via lock on door 14, Col. 3, lines 18-20), and to respond to said control signal by releasing said lid from said complete engagement (via lock on door 14 may be unlocked in response to correct code received, Col. 5, lines 1-5).

Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally. (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose having a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of

Kim to include a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

Regarding claim 24, Kim discloses a data cable coupling said host computer to said port (via communication device 18 may be a line connector, Col. 3, lines 22-26).

16. Claim 25 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Holtkamp as applied to claim 24 above, and further in view of Cayne et al. (US 6,806,807)

Regarding claim 25, the combination of Kim and Holtkamp did not specifically disclose the container manager further comprises a local area network coupling said host computer to said port. Cayne teaches using a local area network to couple a container manager to a host computer (See Fig. 8; and Col. 8, lines 19-21). From the teachings of Cayne, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include the container manager further comprises a local area network coupling said host computer to said port as taught by Cayne to use a LAN for data communication, thereby reliably send/receive data to the container manager.

Regarding claim 26, Kim discloses said port comprising a first antenna mounted within said container (via communication device 18 may comprise an antenna, See Col. 3, lines 22-27); a data transceiver connecting said first antenna and said controller (via transceiver device 226, col. 3, lines 48-51). Kim teaches using the first antenna but did not specifically disclose a second antenna driven by said host computer, operationally connecting said host computer to said first antenna. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim, Holtkamp, and Cayne to include a second antenna driven by said host computer, operationally connecting said host computer to said first antenna in order to use wireless communication between said container and said host computer, thereby making communication easier without the hassle of wires.

17. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Holtkamp, and Cayne et al. as applied to claim 26 above, and further in view of Whiteside (US 5,835,861).

Regarding claim 27, Kim discloses using wireless communication (See Col. 3, lines 22-27), but did not specifically disclose an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data key; and an infrared receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter.

Whiteside teaches using infrared transmitters to broadcast a signal from one device to another device. (See Col. 2, lines 13-19)

From the teachings of Whiteside, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim, Holtkamp, and Cayne to include an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data key; and an infrared receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter as taught by Whiteside to use infrared wireless technology to broadcast/receive a signal from one device to another device, as it is well known infrared signals are less likely to be picked up by unauthorized receivers because infrared signals are direction based, thereby making wireless communication more secured.

Regarding claim 28, the combination of Kim, Holtkamp, Cayne, and Whiteside discloses the container manager further comprising: a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key From said infrared transmitter (see rejection on claim 27 above), and to transmit operational communications from said controller to said host computer via said first infrared transmitter and receiver (See Kim, via communication device 18 to provide output to the safe system 10, Col. 3, lines 22-27).

18. Claims 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim (US 6,040,771), and further in view of Holtkamp (WO 00/76378) and Mogi et al. (JP 06085912 A).

Regarding claims 29-32, Kim discloses a container manager, comprising: a housing comprised of a plurality of sidewalls beating a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, said housing providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement (See Fig. 1); a port exposed through said housing to receive data signals (via communication device 18, Col. 3, lines 22-26); a control stage comprised of a memory (via control stage comprising CPU 220 and memory 204, Col. 3, lines 42-47), said control stage being mounted on said container and being operationally coupled to provide communication by data signals with said interior via said port (Fig. 1). Kim teaches safe systems may be computer controlled, and said port is configured to receive controls signals externally. (See Col. 1, lines 11-13, Col. 3, lines 18-26, Col. 4, line 66 to Col. 5, line 6). But Kim did not specifically disclose a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract) From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the container manager of Kim to include a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

Kim teaches using sensors to detect abnormal conditions (See Col. 4, lines 1-12). But the combination of Kim and Holtkamp did not specifically disclose an alarm driven in response to an unauthorized interruption of said communication via said port to broadcast an indication of said unauthorized interruption in response to said alarm signal. Mogi teaches a communications line sensor to detect unauthorized interruption of the communication line. (See the Abstract) From the teachings of Mogi, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include an alarm driven in response to an unauthorized interruption of said communication via said port to broadcast an indication of said unauthorized interruption in response to said alarm signal in order to prevent theft or tampering of the safe system, thereby improving security.

19. Claims 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim, in view of Holtkamp and Mogi et al. as applied to claim 29 above, and further in view of Campo et al. (US 2003/0104866).

Regarding claim 33, the combination of Kim, Holtkamp, and Mogi discloses the claimed invention wherein Kim discloses said data signals exhibiting a first wavelength (via data signals transmitted wirelessly from an antenna and received by communication device 18), and said data signals exhibiting a second and different wavelength carrier signal (via data signals converted into digital signals by communication device 18 to be processed by CPU 220); and said port comprising a receiver stage converting said data signals into input signals exhibiting said second wavelength (via communication device 18), and a transmitter stage converting said data signals into output signals exhibiting said first wavelength (via transmitter from host computer, See Kim in view of Holtkamp on claim 29 above). But Kim did not specifically disclose said port being plug coupleable to said control stage. Campo teaches the use of removable wireless or wired communications modules on a device (See Paragraph 54). From the teachings of Campo, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim, Holtkamp, and Mogi to include said port being plug coupleable to said control stage as taught by Campo to use removable communication modules, thereby making the system more versatile.

Regarding claim 34, the combination of Kim, Holtkamp, Mogi, and Campo discloses said port comprising: a first unit that is plug coupleable to said control stage when said data signals received by said pot exhibit a first wavelength and said data signals provided by said control stage exhibit a second and different wavelength carrier signal, said first unit comprising a receiver stage converting said data signals received by said port into input signals exhibiting said second wavelength, and a transmitter

stage converting said data signals provided by said control stage into output signals exhibiting said first wavelength (see rejection on claim 33 above). Campo further discloses a second unit that is plug coupleable to said control stage and interchangeable with said first unit to provide a data connection between said control stage and said host computer when said data signals received by said port exhibit the same wavelength as said data signals provided by said control stage (via wired communication module, See paragraph 54 of Campo and rejection on claim 33 above).

20. Claims 38-39, 43 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Holtkamp (WO 00/76378).

Regarding claim 38, Kim did not specifically disclose said control stage generating said control signal in response to instructions received by said control stage from a host computer independently of said disposition of said port, independently of said information represented by said input signal, and independently of said occurrence of coincidence.

Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said control stage generating said control signal in response to instructions received by said control stage from a host computer independently of said

disposition of said port, independently of said information represented by said input signal, and independently of said occurrence of coincidence as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

Regarding claims 39 and 43, Kim discloses said control stage generating said control signal in dependence of said disposition of said port, in dependence of said information represented by said input signal, in dependence of said occurrence of coincidence (See Col. 4, lines 1-12). But Kim did not specifically disclose said control stage generating said control signal in response to instructions received from a host computer coupled to said port. Holtkamp teaches that a secured box may include a communication unit communicating with a computer through a network so that an electrically controlled lock in the delivery box can be opened by a signal from the computer when the input user code matches a valid user code stored. (See the Abstract)

From the teachings of Holtkamp, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said control stage generating said control signal in response to instructions received from a host computer coupled to said port as taught by Holtkamp to remotely input codes on a computer to remotely open the container, thereby making the operation of the container manager more convenient.

21. Claims 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Bates (US 6,583,713) and Heath (5,321,242).

Regarding claims 40-42, Kim did not specifically disclose said container being transportable between an origin and a destination. Bates teach that secured containers may be transported from an origin to a destination (See the Abstract). From the teachings of Bates, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said container being transportable between an origin and a destination as taught by Bates to transport articles securely from one area to another.

The combination of Kim and Bates did not specifically disclose said data key being encoded and being available only at destination. Heath teaches using an access code that is unique to a particular secured location to access a secured device. (See Col. 3, lines 52-57). From the teachings of Heath, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Bates to include said data key being encoded and being available only at destination as taught by Heath to provide access only at a particular location, thereby improving security.

22. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of Holtkamp as applied to claim 43 above, and further in view of Park (US 6,850,149).

Regarding claim 44, the combination of Kim and Holtkamp did not specifically disclose said host computer comprising a cellular telephone bearing a graphical user interface. Park teaches a host computer comprising a cellular telephone bearing a graphical user interface to remotely control devices (via external communication equipment 110). (See Col. 3, lines 22-36 and Fig. 2)

From the teachings of Park, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Holtkamp to include said host computer comprising a cellular telephone bearing a graphical user interface as taught by Park to remotely control devices using a portable device, thereby making remote control more convenient.

23. Claims 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Park (US 6,850,149).

Regarding claim 45, Kim did not specifically disclose some of said data signals being transmitted across Internet. Park teaches a host computer comprising a cellular telephone bearing a graphical user interface to remotely control devices across the internet (via external communication equipment 110). (See Col. 3, lines 22-36 and Fig. 2)

From the teachings of Park, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include some of said data signals being transmitted across Internet as taught by Park to remotely control devices by linking the devices to the internet, thereby making remote control more convenient.

Regarding claim 46, Kim didn't specifically disclose said data signals comprising an e-mail packet. Park teaches a host computer comprising a cellular telephone bearing a graphical user interface to remotely control devices across the internet (via external communication equipment 110). (See Col. 3, lines 22-36 and Fig. 2) The internet is well known to use emails to send/receive data. From the teachings of Park, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said data signals comprising an e-mail packet in order to send data signals across the internet to remote control the container manager, thereby making remote control more convenient.

24. Claim 47 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Cassidy et al. (5,615,625).

Regarding claim 47, Kim did not specifically disclose said information represented by said source comprising a global location of the container, and said control stage generating said control signal in dependence of said disposition of said port, in dependence of said information represented by said input signal, and in dependence of said occurrence of coincidence. Cassidy teaches a container is provided with a global positioning system (GPS) receiver or another positioning system, coupled with a transmitter which transmits the position of the container to a monitoring station, so that the position of the container is monitored closely. (See Col. 5, lines 56 to Col. 6, line 4) From the teachings of Cassidy, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said source comprising a global location of the container, and said

control stage generating said control signal in dependence of said disposition of said port, in dependence of said information represented by said input signal, and in dependence of said occurrence of coincidence as taught by Cassidy to monitor the position of the container, thereby increasing security.

25. Claim 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Bates (US 6,583,713) and Bulfer et al. (5,736,932).

Regarding claim 48, Kim did not specifically disclose said container being transportable between an origin and a destination. Bates teach that secured containers may be transported from an origin to a destination (See the Abstract). From the teachings of Bates, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said container being transportable between an origin and a destination as taught by Bates to transport articles securely from one area to another.

The combination of Kim and Bates but did not specifically disclose a user at said origin requests via a network a request for some part of said data key. Bulfer teaches security for controlled access systems comprising a user request via a network to gain access to the secured system. (See the Abstract) From the teachings of Bulfer, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Bates to include a user at said origin requests via a network a request for some part of said data key as taught by Bulfer to gain access to a secured system remotely with better security.

26. Claims 49 and 55 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Bates (US 6,583,713) and Algazi (US 2002/0091537).

Regarding claim 49 and 55, Kim did not specifically disclose said container being transportable between an origin and a destination. Bates teach that secured containers may be transported from an origin to a destination (See the Abstract). From the teachings of Bates, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said container being transportable between an origin and a destination as taught by Bates to transport articles securely from one area to another.

The combination of Kim and Bates did not specifically disclose said second class of information is installed at said origin comprises biometric data matching a person of a human user of said container and said coincidence must be made with biometric data matching said person at said destination. Algazi teaches using biometric data matching a person of a human user to securely obtain a package in a container (See the Abstract). From the teachings of Algazi, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Kim and Bates to include said second class of information is installed at said origin comprises biometric data matching a person of a human user of said container and said coincidence must be made with biometric data matching said person at said destination as taught by Algazi to provide access to secured devices using biometric data, thereby improving security.

27. Claim 50 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Bates (US 6,583,713).

Regarding claim 50, Kim did not specifically disclose components of said data signals may result in the configuration of container software features. Bates teaches a container with programmable controller to grant access to the user based on factors such as location and time. (See Col. 4, lines 37-45) From the teachings of Bates, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include components of said data signals may result in the configuration of container software features as taught by Bates to make the container manager more versatile to provide access to users.

28. Claim 51 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above, and further in view of Park (6,850,149).

Regarding claim 51, Kim did not specifically disclose said control stage comprises a portable computer and said portable computer provides data to a host computer when said host computer is equipped with a web browser. Park teaches using a portable computer (via external communication equipment 110) to control devices, and the portable device provides data to a host computer when said host computer is equipped with a web browser (via communication equipment 140, Fig, 2, and Col. 3, lines 22-36). From the teachings of Park, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said control stage comprises a portable computer and said portable computer provides data to a host computer when said host computer is

equipped with a web browser as taught by Park to remotely control devices, thereby improving convenience.

29. Claim 52-54 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 1 above, and further in view of Bonner et al. (2002/0153994).

Regarding claim 52, Kim did not specifically disclose a plurality of portable containers is releasably stored in a secured stationary room, the room having a door and a door lock. Bonner teaches a secured stationary room to control access to a designated area. (See paragraph 15) From the teachings of Bonner, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include a plurality of portable containers is releasably stored in a secured stationary room in order to provide more space if one container is not enough, and the room having a door and a door lock in order to control access to a designated area, thereby improving security.

Regarding claim 53, the combination of Kim and Bonner discloses the claimed invention wherein Bonner discloses the door lock is operationally coupled to a port (via control unit 26) to provide communication with a remote control (via programming unit 14). (See paragraph 17 and Fig. 1)

Regarding claim 54, Kim discloses portable containers may be electro-mechanically released (via control signal to electrically unlock container, See Col. 1, lines 51-61).

30. Claim 56 rejected under 35 U.S.C. 103(a) as being unpatentable over Kim as applied to claim 36 above.

Regarding claim 56, Kim did not specifically disclose said housing and said lid may be a housing and drawer. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the container manager of Kim to include said housing may be a housing and drawer as drawers are commonly found in containers to provide retrieval of articles.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONG HANG JIANG whose telephone number is (571)270-3024. The examiner can normally be reached on M-F 9:30 am to 6:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian A. Zimmerman can be reached on 571-272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. J./
Examiner, Art Unit 2612

/Brian A Zimmerman/
Supervisory Patent Examiner, Art Unit 2612